世界知的所有権機関
国際事務局

PCT

特許協力条約に基づいて公開された国際出願

(51) 国際特許分類6
G09C 1/04, 1/00, H04L 9/32

A1

(11) 国際公開番号 WO00/45358

(43) 国際公開日 2000年8月3日(03.08.00)

(21) 国際出願番号 PCT/JP99/01350

(22) 国際出願日 1999年3月18日(18.03.99)

(30) 優先権データ
特願平11/19399 1999年1月28日(28.01.99) JP

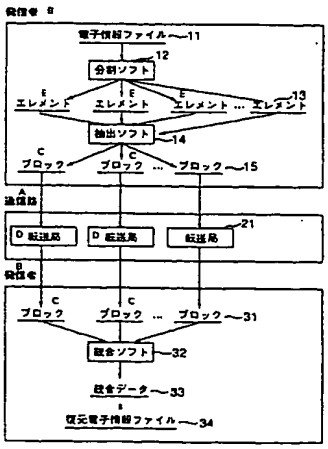
(71) 出願人；および
(72) 発明者
保倉 豊(YASUKURA, Yutaka)[JP/JP]
〒276-0025 千葉県八千代市勝田台南二丁目15番22号
Chiba, (JP)
(74) 代理人
関 正治(SEKI, Masaharu)
〒102-0076 東京都千代田区五番町4番地 幸ビル4階
関特許事務所 Tokyo, (JP)

(81) 指定国 AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW, 欧州特許 (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI特許 (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG), ARIPO特許 (GH, GM, KE, LS, MW, SD, SL, SZ, UG, ZW), ユーラシア特許 (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM)

添付公開書類
国際調査報告書

(54)Title: METHOD FOR SECURING SAFETY OF ELECTRONIC INFORMATION

(54)発明の名称 電子情報の安全確保方法



11...ELECTRONIC INFORMATION FILE
12...DIVIDING SOFTWARE
E, 13...ELEMENT
14...EXTRACTING SOFTWARE
C, 15, 31...BLOCK
D, 21...TRANSFERT STATION
32...INTEGRATED SOFTWARE
33...INTEGRATED DATA
34...RESTORED ELECTRONIC INFORMATION FILE
A...COMMUNICATION CHANNEL
B...SENDER

(57) Abstract

A method for securing safety of electronic information, in which an electronic information file (1) is divided into information elements (2), the information elements are combined in a different order to produce one or more information blocks (3), information element division/extraction data is generated to produce an information block and store or transmit it, the information blocks (3) are divided into information elements (4) again based on the division/extraction data when the electronic information is used, the information elements (4) are arranged in the correct order and integrated to restore the original electronic information file (5), thus resulting in diminishing the value of the information not to be used even if the electronic information stored or being transmitted is stolen.

(57)要約

電子情報ファイル１を複数の情報エレメント２に分割し、分割された情報エレメントを選択し順序を変えて組み合わせることにより１個以上の情報ブロック３を生成し情報エレメントの分割抽出データを生成して情報ブロックを形成して格納もしくは伝送し、電子情報を使用するときに分割抽出データに基づいて情報ブロック３内の情報エレメント４を再分割し、正しい順序に並べ直して統合することにより、元の電子情報ファイル５を復元するようにして、保管中や通信中の電子情報が窃取されることがあってもその情報価値を減殺して利用できないようにした電子情報の安全確保手法。

明細書

電子情報の安全確保方法

技術分野

この発明は、電子情報の保管あるいは電子情報の交換における電子情報の安全確保方法に関し、また電子情報の原本との同一性を保証する方法に関する。

背景技術

多数のコンピュータが通信網に接続されてシステムを形成するようになって、各コンピュータが通信路を介して不特定多数の人と連結されうるようになってきた。このため、ハードディスク装置などコンピュータの外部記憶装置に格納した電子情報も通信路を介して権原のない他人にアクセスされて盗用や改竄をされる心配がある。

また、電子メールその他の個人情報交換、ゲームプログラムやビジネスプログラムなどのアプリケーションプログラムの配布、データベースから抽出編集されたデータの配布など、電子情報を通信路を用いて伝送することが多くなってきた。このような電子情報交換に外部に解放された通信環境を使用する場合には、傍受あるいは窃盗行為などにより受信者でない他人が通信中の電子情報を入手して利用する可能性がある。特に有料で情報を配布する場合やプライバシーに係わる情報を伝送する場合には、通信中の電子情報を容易に盗用されないようにする必要がある。

無関係の他人が電子情報を入手しても利用できなくするため、暗号化することにより電子情報の秘密性を確保する方法が行われている。このような目的に開発された暗号化技術は、対称鍵を用いた暗号方式、非対称鍵を用いた暗号方式、それぞれ多様に存在する。

しかし、これら暗号化技術を用いても、保管されている電子情報や伝送されている電子情報には全ての情報が含まれているため、暗号の解読など何らかの手段で復号方法を入手した者があれば、容易に復元して有用な情報を入手することができる。また、情報の改竄や偽造も可能で、取り出したり受け取った電子情報が

真正な情報を維持しているか否かを常に心配しなければならない。特に本人認証データなど、高い秘匿性が要求される電子情報を保管したり伝送する場合に、従来方法では不安がある。

保管中や通信中に改変を受けたり情報の欠落があった場合には、取出しあるいは受信した情報の多くは正しい利用ができなくなり、また正しくない情報をそのまま使用して不都合を招来する場合もある。また、情報が第三者に知られること自体が問題となる場合がある。したがって受信した電子情報が送り出したものとの同一性を保持していることを確認するため、また電子情報が正当に使用されることを確認するための便利な手法が要求される。

そこで、本発明は、保管や伝送をしようとする電子情報を加工して、たとえ保管中や通信中の電子情報が窃取されることがあっても利用できないようにして情報価値を減殺することにより電子情報の安全を確保する手法を提供することを目的とし、また使用者が取り出しあるいは受信して復元しようとする情報の真正性を保証する方法を提供することを目的とする。

発明の開示

本発明の電子情報の安全確保方法は、電子情報ファイルを複数の情報エレメントに分割し、分割された情報エレメントを選択し順序を変えて組み合わせることにより1個以上の情報ブロックを生成する。この情報ブロックは、全ての情報ブロックを統合すると全ての情報エレメントが含まれるようにする。さらに情報エレメントへの分割方法と情報ブロックの形成方法を記録した分割抽出データを生成し、情報ブロックおよび分割抽出データを保管もしくは伝送する。そして、電子情報を使用するときに、すべての情報ブロックと分割抽出データを集合し、分割抽出データに基づいて情報ブロック内の情報エレメントを再分割し、正しい順序に並べ直して統合することにより、元の電子情報ファイルを復元することを特徴とする。

なお、分割抽出データを別途に格納もしくは送付するようにしてもよく、また、各情報エレメントに係る分割抽出データを生成して情報エレメント毎に付帯させてもよい。

本発明の電子情報の安全確保方法によれば、保管あるいは送付すべき電子情報ファイルを適当な数の適当な長さの情報エレメントに分割した上でシャッフルして組み合わせることにより１個以上の情報ブロックを形成し、この情報ブロックを外部記憶装置に格納しあるいは受信者に送付する。

したがって、保管中あるいは通信中の電子情報はシュレッダにかけられた紙情報と同様に復元しない限り役に立たない状態になっているので、復元手段を持たない他人がアクセスしても価値を有する情報として漏洩する訳ではなく安全である。

電子情報ファイルに対して１個の情報ブロックしか形成しない場合でも、情報ブロック内に収納された情報エレメントの順序が入れ替わっているため情報を判読することが困難である。しかし、複数の情報ブロックを形成してそれぞれを別々に保管あるいは送付するようにすれば、たとえ他人が一部の情報ブロックを盗窃しても電子情報の全容が盗まれることにはならないので、より安全性が向上することはいうまでもない。

また、情報ブロックはさらに暗号技術を適用して保管あるいは送付するようにして、格段の安全性向上を図ることもできる。

分割抽出データは、情報ブロックを形成するときに用いられた分割・組合わせに必要なデータであって、情報ブロックと共に格納あるいは送付する。分割抽出データは情報エレメント毎の電子情報ファイルにおける位置情報や長さ情報を含むものであるから、情報エレメント毎に付帯させておいて情報ブロックと一緒に扱っても良い。また、安全性を重視する場合には情報ブロックとは別途に扱うようにしても良い。

電子情報を取り出す者や受信する者は全部の情報ブロックを集め、分割抽出データを使用して、各情報ブロックに含まれる情報エレメントをそれぞれに分離し、正しい順に再結合して元の電子情報に復元する。

コンピュータの外部記憶装置に電子情報を記憶させるときに、電子情報ファイルを上記のように処理して情報ブロックと分割抽出データを生成して、これらを外部記憶装置に記憶させるようにしてもよい。

本発明の安全確保方法を記憶装置に適用することにより、他人のアクセスがあ

っても価値ある情報の流出には結びつかず、コンピュータにおける電子情報保管の安全性が向上する。

なお、電子情報を送付するときには、電子情報ファイルを複数の情報エレメントに分割し、分割された情報エレメントを選択し組み合わせて複数の情報ブロックを形成して、情報ブロックのそれぞれを分離した状態で受信者に伝送すると共に分割抽出データを受信者に伝送し、これらのデータを受け取った受信者側で分割抽出データに基づいて情報ブロックに含まれる情報エレメントを再分割し正しい順に統合して元の電子情報に復元するようにすることが好ましい。

電子情報ファイルを送付するときは使用する通信路が広く一般に解放されていることがあるため、より高度な安全性を有することが好ましい。このような場合にも、複数の情報ブロックを異なる通信手段で送付するようにすることにより格段に高い安全を確保することができる。

本発明における情報ブロックはそれぞれ必要な情報の一部を搭載しているだけなので、たとえ通信途中で一部の情報ブロックを入手しても情報の全体を復元することはできない。

したがって、情報ブロックおよび分割抽出データのうち少なくとも１個を他の電子情報の伝送手段と異なる第２の伝送手段により受信者に送付するようにすることが好ましい。

情報ブロックおよび分割抽出データを全て同じ伝送手段を用いて送付しないで、そのうちのいくつかを異なる伝送手段により送付する場合は、通信路途中に窃取者が存在しても全部の情報を集めることができないので、より安全である。

情報ブロックをそれぞれ異なる時刻に送ったり、別の通信ルートを使用して送るようにすれば、通信路の途中で全ての情報ブロックを漏らさず窃取することは非常に困難であり、せいぜい情報の一部を入手できるだけであるから、たとえば本人認証データを送付する場合にも、他人がこれを盗用することを避けることができる。

なお、分割抽出データには電子情報ファイルの原本性を確認するデータを含ませることが好ましい。送付しようとした電子情報ファイルと受信者が復元した電子情報が同一のものであることは、分割抽出データと受け取った情報ブロックの

内容が矛盾していないことを検証することにより高い確度で確認することができる。

また、送付しようとした電子情報ファイルと受信者が復元した電子情報が同一のものであることは、別の通信ルートで送付される情報ブロックに情報エレメントの内から選択した情報エレメント、すなわちキーエレメントが共通して含まれるようにして、情報エレメントを統合するときに受信した情報ブロックに重複して含まれているキーエレメント同士の同一性を検証することにより確認するようにしてもよい。

なお、送付された電子情報ファイルが送付しようとした電子情報ファイルと同じ物であることを確認するためには、それぞれのファイルに含まれる語数が一致しているか否かを調べるという簡単な方法もある。

本発明の電子情報の安全確保方法をアプリケーションプログラムやデータベースのオンライン販売に用いれば、正当な購買者以外の者が通信中の電子情報を窃取しても一部の情報しか入手できないので、プログラムを実行することができず、また有用な情報を取得することができない。したがって通信中の電子情報を窃取する動機がないため、販売者の利益が窃取により損なわれることがない。

また、本人認証データを送付するために適用すれば、他人の盗用や偽造を確実に防止して、安全性の高い情報交換ができる。

さらに厳格な保証が必要なときには、送付する電子情報の原本を保存し、受信者側で復元した電子情報を返送させ、電子情報原本と照合して同一性を確認するようにすることが好ましい。

さらに、受信者が復元した電子情報を返送させ、保存してある電子情報原本と照合して同一性を確認するようにすれば、通信の途中で改竄されたり通信情報の一部が欠落したりした場合にも直ちに判定して対策をとることができる。

なお、受信者が入手した情報ブロックをそのまま返送させて電子情報原本と照合するようにしてもよい。情報ブロック毎に検査することにより障害を受けた部位を特定することができ、対策が容易になる。

原本と差異がある場合は、通信路の信頼性を疑って再度情報を送付したり、改竄者の介入を回避して通信路を変更したりすることができる。なお、受信者も送

信者からの照合結果を受け取ることにより安心して電子情報を利用することができる。

伝送手段中に中立的で公正な転送局を配設し、転送局を介して情報伝送を行うようにすると信頼性が向上する。転送局は自局宛に送られた情報パッケージに含まれる情報ブロックを宛先情報に基づいて受信者に転送する。

このようなルートを使用して情報ブロックを送付する場合は、分割された情報ブロックの外見がそれぞれ異なるため、通信路途中の窃取者が電子情報ファイルを復元するために必要となる情報ブロックを全て収集することが困難になり、安全性はさらに向上する。

特に、分割抽出データを含む部分を転送局を介して送付するようにしただけでも、システム全体の信頼性が向上する。

なお、転送局が暗号技術を適用して電子情報を転送するようにすれば、より高度な安全性を確保することができる。

また、送信された情報は必ずしも受信者が直ちに使用するとは限らない。そこで送信者が送付した情報ブロックを転送局で保管しておいて、受信者が必要に応じて転送局に情報ブロックを送信させ、収集した情報ブロックを統合し復元して利用するようにしても良い。

さらに、当事者間の争いを避けるため証明局を介在させて電子情報の同一性を保証するシステムを利用する場合にも、電子情報ファイルを分割して得られる情報ブロックを証明局と当事者がそれぞれ分かち持つようにして、電子情報を使用するときに証明局と当事者とから関連する情報ブロックを収集し統合して元の電子情報に復元するようにして、電子情報の安全性を保証するようにすることができる。

この方法では、本発明の電子情報の安全確保方法を利用し、情報の一部を証明局に預けておいて元の情報を必要とするときに手元の情報ブロックと相手の所有する情報ブロックに加えて証明局に預けた情報ブロックを合わせて復元するようにする。したがって、当事者と証明局のいずれが情報を改竄しても改竄の事実が明確に分かる上、証明局が保管するのは情報全体でなく一部であるので、証明局の備えるべき情報容量は小さくて良い。また、情報の安全性を認証する機能が三

者に分割されているため証明局としての負担も少ないことが証明局運営上の利点となる。

図面の簡単な説明

第１図は本発明の電子情報の安全確保方法の概念を説明するブロック図、第２図は本発明の１作用を説明する図面、第３図は本発明の電子情報の安全確保方法に係る第１実施例を表すフローダイヤグラム、第４図は本実施例を使用したシステムのブロック図、第５図は本発明の電子情報の安全確保方法に係る第２実施例を表すフローダイヤグラム、第６図は本実施例を使用したシステムのブロック図、第７図は本発明の電子情報の安全確保方法に係る第３実施例を表すフローダイヤグラム、第８図は本実施例を使用したシステムのブロック図、第９図は本発明の電子情報の安全確保方法に係る第４実施例を表すフローダイヤグラム、第１０図は本発明の電子情報の安全確保方法に係る第５実施例を表すブロック図、第１１図は本発明を適用した証明局の機能を説明するブロック図である。

発明を実施するための最良の形態

本発明の電子情報の安全確保方法は、電子情報ファイルの保管あるいは通信において電子情報の安全を確実にする方法である。本発明の方法により、保管中や通信途中で電子情報を窃取する者があっても窃取によって入手できる情報の有する価値を小さくして窃盗の被害を防ぐと共に、窃盗の利益を減殺したことにより窃取行為を予防し、また通信中に情報の欠落や情報の改竄があったときにはその事実を検知するようにして安全性を確保する。

以下、図面を参照して本発明の詳細を説明する。

第１図は本発明の概念を説明するブロック図、第２図は発明の１作用を説明する図面である。第１図は、本発明の使用態様の１例として、電子情報ファイルを６個の情報エレメントに分割し２個の情報ブロックに分けた場合を示している。

本発明の電子情報の安全確保方法では、対象とする電子情報ファイル１を適当な数の情報エレメント２に分割する。ここでは、簡単のため、６個の情報エレメントＡ，Ｂ，Ｃ，Ｄ，Ｅ，Ｆに分割する場合を例として説明している。情報エレ

メント２は情報として意味がある位置で区切る必要はなく、盗用される可能性を少なくするためには、電子情報ファイル１を単に物理的に分割したものである方が好ましい。

分割した情報エレメントＡ，Ｂ，Ｃ，Ｄ，Ｅ，Ｆの配列順を変更し適当にグループ化して適当数の情報ブロック３を形成する。

図示した例では、第１の情報ブロック３に情報エレメントＡ，Ｄ，Ｅを配分し、第２の情報ブロック３に情報エレメントＢ，Ｃ，Ｆを配分している。なお、情報ブロック３内の情報エレメントの配列順も任意に変更することができる。

このような情報ブロック３を他人が読み出しても、情報エレメントＡ，Ｂ，Ｃ，．．．が意味のある配列になっていないため、そのままでは電子情報の内容を読みとることができない。

また、電子情報が分割されているため、全ての情報ブロックを入手しないと内容を復元できない。たとえば第２図（ａ）に示す本人認証データを第２図（ｂ）に示すように分割したときには、一方の情報ブロックを入手して復元に成功しても、認証データとして利用することができない。このため不正にアクセスする者がいても電子情報を利用できるようにすることは容易でなく、情報の安全を保持することができる。

この情報ブロック３を目的に応じて記憶装置に保管し、あるいは受信者に送付する。

電子情報の使用者は保管先から取得したり送信者から受信した情報ブロック３を元の情報エレメント４（Ａ，Ｂ，Ｃ，．．．）に分割し、これらを正しい順序に並べ直して使用可能な電子情報ファイル５に戻すことにより元の電子情報ファイル１を復元する。

電子情報ファイル１を復元するために必要となる基礎的な情報は、各ブロック３に含まれる情報エレメントＡ，Ｂ，Ｃ，．．．の区切り情報と、各情報エレメントの電子情報ファイル１における位置と長さの情報である。

目的の電子情報ファイル１に関連する情報ブロック３を全て収集した上で、情報ブロック３内の情報エレメントを切り出し、各情報エレメント２の先頭番地と語長の情報を用いて、正しい順に並べ直すことができる。

また、電子情報ファイル１を復元するときに、目的の電子情報ファイル１を特定する情報や、情報エレメント２を並べ替えて情報ブロック３を形成したときの各ブロックに含まれる情報エレメントの配列順序の情報を利用してもよい。

電子情報ファイル１を復元するときには、まず、集めた情報ブロック３が目的の電子情報ファイル１に関連するものであり、関連する全ての情報ブロックが落ちなく集まっていることを確認する必要がある。このとき、情報ブロックや情報エレメントに識別領域Ｘ１，Ｘ２を付帯させ、この識別領域に電子情報ファイル１を特定するＩＤ情報を記載して利用すると効率よく作業ができる。

また、区切り情報を用いて各ブロックに含まれる情報エレメントを再分割し、さらに分割された情報エレメント４の配列順にしたがって再配列して得た電子情報ファイル５は元の電子情報ファイル１と同じ物となる。

なお、復元した電子情報ファイル５と元の電子情報ファイル１が同じ物であるか否かは、たとえば両者の総語長を比較することで、ある程度の確度をもって検証することができる。

これらの基礎的情報を含む分割抽出データは、情報ブロック３を形成するときに作成されて、情報ブロック３の一部に識別領域を添付して格納あるいは送付され、電子情報ファイル１を復元するために利用される。分割抽出データは、情報エレメント毎に添付するようにしてもよい。

なお、分割抽出データは情報ブロック３とは別途独立に保管あるいは送付されるようにしても良い。

本発明の電子情報の安全確保方法では、１個の電子情報ファイル１に対応する情報ブロック３は２個に限らず、３個以上の複数でもよく、また１個であっても良い。いずれも情報ブロック３内の情報エレメントの配列が元のものと異なるため他人が読み出して利用することができないので電子情報の安全を保持することができる。

（実施例１）

第１の実施例は、本発明の電子情報の安全確保方法を適用して、電子情報ファイルを通信路を使用して安全に相手方に送信するものである。

第３図は本実施例を表すフローダイアグラム、第４図は本実施例を使用するシ

ステムのブロック図である。

まず、第３図と第４図を参照して本実施例の基本的な態様について説明する。

電子情報の発信者は、まず送信しようとする電子情報に関係して、新たに作成したりデータベースから抽出して編集することにより、電子情報ファイル１１を準備する（Ｓ１）。対象になる電子情報の例として、本人認証データのような高度の安全性を要求されるようなものや、通信路を介して販売されるソフトウエアなど有価のものなどがある。

次に、分割ソフト１２を用いて電子情報ファイル１１を複数の情報エレメント１３に分割する（Ｓ１２）。分割ソフト１２には情報エレメント１３のおのおのに関して電子情報ファイル１１内の分割位置と情報エレメントの語長を指示できるようになっている。

なお、分割位置と語長を各情報エレメント毎に指示する代わりに、分割数を指定すると分割ソフト１２が自身で決定するようにしても良い。分割数は任意に決めることができるが、１００kByte程度までの電子情報を対象にするときにはたとえば１００以内の個数を選択するように決めてもよい。

次に、抽出ソフト１４を用いて情報エレメント１３を複数の情報ブロック１５に配分する（Ｓ３）。抽出ソフト１４は、分割された情報エレメント１３の順番を入れ替えて再配列する機能と、これらを情報ブロック１５に分配する機能を有する。情報ブロック数はオペレータが指示できるようになっている。

また、情報エレメント１３の分割情報および再配列の結果は分割抽出データとして電子情報化し、それぞれ情報エレメント１３に付帯させる。各情報ブロック１５に配分された全ての情報エレメント１３の分割抽出データをまとめて情報ブロック１５の識別領域Ｘ１，Ｘ２に付帯させても良い（Ｓ４）。

なお、識別領域Ｘ１，Ｘ２には、発信者や受信者に関するデータ、制作者や所属など電子情報に関するデータ、利用者や有効期限など電子情報を利用できる範囲を記述したデータ、統合ソフトなど適用するソフトを特定するデータなどを付帯させてもよい。

また、識別領域に電子情報を指示するＩＤを記述しておくと情報ブロックの仕訳が容易になるので、受信者が再統合して電子情報ファイルを復元するために目

的の電子情報に係わる情報ブロックを収集する場合に便利である。

なお、分割抽出データは情報ブロックとは別途独立に受信者に送付するようにしても良い。また、各情報ブロックに分散して付帯させる代わりに、いずれかの情報ブロックにまとめて付帯させても良い。さらには全ての情報ブロックに電子情報ファイル全体に関する分割抽出データを付帯させるようにしても良い。

次に、各情報ブロック１５をそれぞれ転送局２１に送信するためのパッケージに収納する（Ｓ５）。パッケージには最終的に受信するべき者の宛名を収納しておく。このパッケージを暗号処理して転送局２１に送る（Ｓ６）。暗号処理は適当な公知方法を適用して行えばよい。

このとき、パッケージ毎に異なる送り先を選ぶことができる。通信路の危険性や電子情報の性格から決まる安全性の程度に基づいて、使用する通信手段を選択する。漏洩や改竄を極端に嫌う場合はできるだけ多数の通信手段を使用するようにする。

なお、情報漏れの危険が小さいときには転送局が存在しない通常の通信路を使用しても良い。本発明の安全確保方法は、電子情報を分割して再配列した状態で通信路に置くため高い安全性を有するので、通常の通信路を使用しても従来方法と比較して十分安全である。

また、通信手段として、例えば郵便を用いてフロッピーディスクなど可搬の記憶装置を送る方法などを選択することもできる。

パッケージを受け取った転送局２１は、これを復号化して収納された宛先情報を読みとる（Ｓ７）。

次に、パッケージに収納された情報ブロックを再度暗号化して指示された受信者に向けて送付する（Ｓ８）。

このように情報ブロック１５が外見から内容が分からない状態になって別々の転送局に配送されるため、他人が通信路中に存在する電子情報を入手できたとしても、必要な情報を判別して収集することが困難で目的の電子情報を復元することができない。

受信者は転送局から送り込まれた情報ブロック３１を受信して（Ｓ９）復号し、情報ブロックもしくは情報エレメントの識別領域部分をサーチすることにより、

目的の電子情報を復元するために必要となる情報ブロック３１を全て収集する（Ｓ１０）。

また、識別領域部分の分割抽出データから情報エレメント１３を生成したときの分割情報と情報ブロック１５を生成したときの抽出情報を取り出す（Ｓ１１）。

次いで、統合ソフト３２を用いて、分割情報と抽出情報に基づいて情報ブロック３１を再分割し元の情報エレメント１３を切り出し（Ｓ１２）、元の順序に配列し直す（Ｓ１３）。

最後に、全部の情報エレメントを合体し統合して電子情報ファイル３３を形成する。このとき、統合して形成された電子情報ファイル３３の全長を分割抽出データに含まれている元ファイルの全長値と比較する（Ｓ１４）。両者が一致すれば、かなり高い確度で元の電子情報ファイル１１が復元できたとすることができる。さらに、原本の性格を記述する情報や適当なしおりを挿入した位置情報などを用いて原本との同一性をより正確に確認するようにすることも可能である。

（実施例２）

第２の実施例は本発明の電子情報安全確保方法において、さらに高度に電子情報の原本性を保証する手段を備えたものである。

第５図は電子情報の発信者において原本性を確認する手段を備えた第２実施例の電子情報安全確保方法を表すフローダイアグラム、第６図はそのブロック図である。

以下、第５図と第６図により、電子情報の発信者において原本性を確認する手段を備えた本発明の実施例を説明する。

なお、本実施例において基本となる安全確保方法については、既に説明したものと同じであるので、以下ではその部分を簡約したり省略することにより誤解を招かない程度に説明の重複を避けることにする。

発信者は送付すべき電子情報ファイル１１を生成したときに、その原本から写本１７を生成し（Ｓ２１）、写本１７を保存する（Ｓ２２）。なお、写本１７の代わりに原本１１を保存しても同じである。

次に、分割抽出ソフト１６を用いて、既に説明した第１実施例と同じように、操作者から与えられた、あるいは一部コンピュータで生成した分割情報と抽出情

報に基づいて電子情報ファイルの原本１１を加工して情報ブロック１５を形成する（Ｓ２３）。なお、原本１１を保存する場合は加工する対象を写本１７にする。

情報ブロック１５はそれぞれ第１実施例と同じようにして転送局２１宛てに送付する（Ｓ２４）。

転送局２１は、受信した情報ブロック１５を指示された受信者に転送する（Ｓ２５）。

受信者は受信した情報ブロック３１を調べて、目的の電子情報を復元するために必要な情報ブロック３１を全て集める（Ｓ２６）。

次に、取得した分割抽出データに含まれる抽出情報と分割情報に基づき、統合ソフト３２を用いて、各情報ブロック３１内の情報エレメントを抽出し配列順を正して統合し電子情報ファイル３３を形成する（Ｓ２７）。

さらに、形成された電子情報ファイル３３の写本３５を生成し（Ｓ２８）、これを送信と同様の方法で転送局２２を介して電子情報の発信者に返送する（Ｓ２９）。この場合の転送局２２は、送信の場合と同様に複数であることが好ましい。また、返送する電子情報ファイルの写本３５は暗号化処理を施して安全性を高めておくことが好ましい。

発信者は、受け取った復元電子情報ファイルの写本３５と保存しておいた電子情報ファイル写本１７とを比較照合して、同一性を確認する（Ｓ３０）。

両者が一致しない場合は電子情報として使用できないので受信者にその旨を通知する（Ｓ３１）。受信者は発信者からの警報通知を受けない場合は情報ファイルの復元が正常に行われたと判断することができる（Ｓ３２）。

なお、二つのファイルが一致しない場合は、通信中に何らかの障害があったことを示すので、原因を究明して排除し次回以降の通信を安全に行えるようにしなければならない。原因の排除ができない場合は通信手段を変更することが好ましい。

このようにして、受信者における電子情報の復元が正しく行われたことを発信者が確認するようにすることにより、極めて信頼性の高い電子情報交換が実現することになる。

（実施例３）

第３の実施例は、本発明の電子情報の安全確保方法において、情報ブロック毎に原本性を確認する手段を備えて、個々の通信路の異常を検出して対策をより容易にする電子情報の原本性保証方法である。

第７図は本実施例を表すフローダイアグラム、第８図は本実施例を使用するシステムのブロック図である。以下、第７図と第８図により、本実施例を詳細に説明する。

なお、本実施例についても、既に説明したものと同じ部分を簡約したり省略することにより説明の重複を避けることにする。

発信者は、第１実施例におけると同様に、送付すべき電子情報ファイル１１を作成し（Ｓ４１）、分割情報と抽出情報に基づいて情報エレメントを切り出しこれをシャッフルして情報ブロック１５を形成する（Ｓ４２）。

情報ブロック１５から写本を生成して保存しておく（Ｓ４３）。

次に、第１実施例と同じ方法で転送局２１に情報ブロック１５を収納したパッケージを送付すると（Ｓ４４）、転送局２１はパッケージを復号して受信者の宛名を読みとり情報ブロック１５を改めて指定された受信者に転送する（Ｓ４５）。

受信者は受け取った情報ブロック３１の写本を作成して（Ｓ４６）、転送局２３を介して発信者に返送する（Ｓ４７）。

発信者は、返送された情報ブロック３１の写本と保存してある元の情報ブロック１５の写本とを照合して一致するか否かを確認する（Ｓ４８）。

両者が一致するときは通信中に変成を受けなかったのでそのまま使用して電子情報の復元ができる。

また、両者が一致しないときには、その情報ブロックを伝達した通信路に異常があることを示す。上記第２の実施例においては、異常の検出は可能であるが、全ての通信路を統合した形で検出するので、異常のある通信経路を特定することが困難であった。しかし、本実施例における方法を使用すると上記の通り簡単に異常経路を特定することができる。したがってまた、障害の除去などの対策が容易である。

発信者が行った照合の結果は受信者に通知される（Ｓ４９）。

照合の結果、２つの写本が一致するときは統合ソフト３２を用いて第１実施例

と同じ手順で電子情報ファイルの復元を行う（Ｓ５０）。情報ブロック３１から形成された統合データ３３は元の電子情報ファイル１１と同じ内容を持つファイル３４になる。

なお、電子情報の交換は上記のような転送局２１，２３が存在しない通信路を用いて行っても良いことは第１実施例の説明において述べたとおりである。

また、転送局は送信者が送付した情報ブロックを保管しておいて、受信者の要求に従ってその情報ブロックを送信するようにしてもよい。受信者は全部の情報ブロックを収集し、これらを統合し復元して利用する。

（実施例４）

第４の実施例は本発明の電子情報の安全確保方法を適用して、電子情報ファイルをコンピュータシステムの外部記憶装置に保管するものである。

第９図は本実施例の電子情報安全確保方法を使用するコンピュータシステムのブロック図である。

以下、図面を参照して本実施例について説明する。

なお、本実施例における構成要素の作用効果は、上記説明した各実施例におけるものと共通する部分が多いので、上記実施例と同じ機能を備える構成要素部分については同じ参照番号を付し説明を簡約にし、重複を避けている。

コンピュータシステムで作成した電子情報ファイル４１は、分割抽出ソフト４２により情報エレメントに分割して再配列し、複数の情報ブロック４３に配分してから記憶装置５０に格納される。

記憶装置５０から取り出すときは、対象とする電子情報を担持している情報ブロック６１を全て収集し、統合ソフト６２を実行する。統合ソフト６２は情報ブロック６１から分割情報と抽出情報を抽出し、これら情報に基づいて情報ブロック６１内の情報エレメントを切り出し、元の順に配列し直して統合し、電子情報ファイル６３を生成する。

本実施例の電子情報安全確保方法を用いると、記憶装置５０に収納されている電子情報ファイルが複数の情報ブロックに分割されていて、目的の電子情報が復元できるように関係する情報ブロックを全て集めることは難しい。また、情報ブロック内部の情報エレメントもシュレッダにかけられた紙情報のようにバラバラ

になっているので、電子情報の一部を再現することも容易でない。

このようにして、外部からのアクセスにより情報が漏洩することを防止することができる。

なお、記憶装置５０に記録する際に暗号処理を施しても良い。

また、記憶装置５０は１個の記憶装置である必要はなく、情報ブロック毎に別個の記憶装置に保存するようにしても良い。

本実施例の電子情報安全確保方法は、機密性が特に要求される認証局において本人認証データをハードディスク装置や磁気テープ装置など外部記憶装置に保存するときに適用することができる。

（実施例５）

第５の実施例は本発明の電子情報の安全確保方法において、電子情報の一部を利用して電子情報の原本性を保証する手段を備えたものである。第１０図は、本実施例に用いた原本性保証手段を説明するブロック図である。本実施例において基本となる電子情報の安全確保方法については、既に説明したものと同じであるので、以下ではその部分を簡約して説明の重複を避けることにする。

第１０図は、本発明の使用態様の１例として、電子情報ファイルを７個の情報エレメントに分割し２個の情報ブロックに分けた場合を示している。

分割した情報エレメントＡ，Ｂ，Ｃ，Ｄ，Ｅ，Ｆ，Ｇは配列順を変更し適当にグループ化して２個の情報ブロックに配分される。このとき、情報エレメントの内のいくつかはキーエレメントとして両方の情報ブロックに共通して含まれるようにする。また、情報ブロックには情報エレメントの区切り情報と電子情報ファイルにおける位置と長さの情報と電子情報ファイルのＩＤ情報などを記録した識別領域Ｘ１，Ｘ２を付帯させて復元のために利用できるようにしておく。

第１０図に図示した例では左の情報ブロックに情報エレメントＡ，Ｂ，Ｃ，Ｅ，Ｆが配分され、右側の情報ブロックには情報エレメントＢ，Ｄ，Ｅ，Ｇが配分されていて、情報エレメントＢとＥがキーエレメントとしていずれの情報ブロックにも含まれている。各情報ブロック中の情報エレメントは適当に順位が入れ替わっていて意味のある配列になっていないため、情報ブロックを他人が読み出してもそのままでは電子情報の内容を読みとることができない。この情報ブロックは

目的に応じて記憶装置に保管され、あるいは受信者に送付される。

電子情報の使用者は入手した情報ブロックを、識別領域Ｘ１，Ｘ２に記録された情報に基づいて、元の情報エレメント（Ａ，Ｂ，Ｃ，．．．）に分割しこれらを正しい順序に並べ直して元の電子情報ファイルを復元する。

復元時には、２つの情報ブロックに重複して含まれキーエレメントとなっている情報エレメントＢ，Ｅを検出して照合する。すると、いずれかの情報ブロックが情報の保管時あるいは伝送時に何らかの改変を受けたときには、重複する情報エレメントの内容が一致しないので簡単に異常の検知ができる。

本実施例に用いた異常検出方法は、情報ブロックを単独に観察しても照合対象とするキーエレメントを抽出することができないので容易に第三者の攻撃を回避することができる。また、特別な付加情報を必要とせず安全性を確認するための情報処理が簡単である。

なお、本実施例の異常検出方法を他の方法と併用して安全性を向上させても良いことは言うまでもない。

（実施例６）

第６の実施例は本発明の電子情報の安全確保方法を適用して、各所に電子情報を分割して保管し、当事者間の取引内容などの照合証明を正確に行う証明局に関するものである。

第１１図は本発明を適用した証明局の機能を説明するブロック図である。本実施例において基本となる安全確保方法は既に説明したものと同じであるので、以下では証明局に用いる部分について丁寧に説明し他の部分については説明の重複を避けることにする。

第１の当事者Ｉと第２の当事者IIは、互いに合意した取引内容を電子情報化して保管する。しかし、電子化された文書は書き換えを行っても痕跡が残らないので原本性は保証できない。したがって、将来の争いの余地を小さくするため信頼を置くことができる第三者の機関である証明局ＣＡを利用して、取引内容を寄託しておき必要に応じて原本の提示を受けて確認するようにすることが要請される。

ところが、原本をフルテキストとして記録する場合は証明局ＣＡには極めて大きな記憶容量が必要となる。また、証明局ＣＡでも改竄を受ける可能性があり、

電子情報の真正性を完全に保証しようとすると証明局ＣＡの管理運営には大きな困難が付いて回ることになる。

本実施例は、本発明の電子情報安全確保方法を適用して構成したもので、証明局ＣＡの負担が小さくしかも高い確度で電子情報の原本性を保証する認証システムである。

当事者Ⅰ，Ⅱは相互の合意内容を前記実施例の方法に基づいて情報ブロックＡ，Ｂ，Ｃに分割する。第１当事者Ⅰは第１の情報ブロックＡを保管し、第２当事者Ⅱは第２の情報ブロックＣを保管する。さらに、第３の情報ブロックＢは証明局ＣＡに寄託する。

当事者間で合意内容に争いがあるときには、両当事者が保管して置いた情報ブロックＡ，Ｃと証明局ＣＡに寄託して置いた情報ブロックＢを統合し当初の合意文書の電子情報を正しく復元して、いずれの主張が正当であるかの認定をすることができる。

このような認証システムでは、いずれかの機関で記録を変成した場合には原本を復元することができない。したがって復元された電子情報は正しく原本の内容を伝えることになる。このため、証明局ＣＡは原本の極く一部を記録しておくだけで復元された電子情報の原本性を保証することができる。このように証明局ＣＡの有するべき記憶容量が小さくなり、また合意内容全文の保管をしなくても良いため証明局ＣＡとしての保管責任も緩和されることになる。

産業上の利用可能性

以上詳細に説明した通り、本発明の電子情報の安全確保方法は、電子情報ファイルを一旦情報エレメントに分割して再配置し情報ブロックに分納して通信路に置いたり記憶装置に納めるので、外部の者が通信途中や格納中の情報ブロックを窃取しても、小さな情報エレメントがバラバラに収納されていて電子情報の内容を判読することができず、秘密の漏洩を防ぐことができる。また、電子情報を復元する際に電子情報の原本性を容易に確認することができる。なお、受信者が通信路を介して受け取った通信結果や復元した電子情報ファイルを発信者まで返送して保存した写本と照合するようにしたものでは原本性を極めて高度に保証することができる。

請求の範囲

1．電子情報ファイルを複数の情報エレメントに分割し、分割された情報エレメントを選択し順序を変えて組み合わせることにより全ての情報ブロックを統合すると全ての情報エレメントが含まれるような1個以上の情報ブロックを生成し、また前記情報エレメントと情報ブロックの形成情報を記録した分割抽出データを生成し、該情報ブロックと分割抽出データを格納もしくは伝送し、該電子情報を使用するときにすべての前記情報ブロックと分割抽出データを集合して該分割抽出データに基づき前記情報ブロックに含まれる情報エレメントを再分割し正しい順序に並べ直して統合し、元の電子情報ファイルを復元することを特徴とする電子情報の安全確保方法。

2．前記分割抽出データを別途に格納もしくは送付することを特徴とする請求の範囲第1項記載の電子情報の安全確保方法。

3．前記各情報エレメントに係る前記分割抽出データを該情報エレメント毎に付帯させることを特徴とする請求の範囲第1項記載の電子情報の安全確保方法。

4．前記情報ブロックと分割抽出データを外部記憶装置に記憶して外部記憶装置における電子情報を安全に保管することを特徴とする請求の範囲第1項から第3項のいずれかに記載の電子情報の安全確保方法。

5．前記情報ブロックを複数形成し、該情報ブロックのそれぞれを分離した状態で前記分割抽出データと共に受信者に伝送することを特徴とする請求の範囲第1項から第3項のいずれかに記載の電子情報の安全確保方法。

6．前記分割抽出データに前記電子情報ファイルの原本性を確認するデータを含ませることを特徴とする請求の範囲第5項記載の電子情報の安全確保方法。

7．前記情報エレメントの内から選択した情報エレメントが複数の情報ブロックに共通して含まれるようにして、情報エレメントを統合するときに別々の情報ブロックに重複して含まれている前記情報エレメント同士の同一性を検証して情報の安全を確認することを特徴とする請求の範囲第1項から第6項のいずれかに記載の電子情報の安全性確保方法。

8．さらに、送付する電子情報の原本を保存し、受信者側で復元した電子情報を返送させ、前記電子情報原本と照合して同一性を確認することを特徴とする請求

の範囲第５項から第７項のいずれかに記載の電子情報の安全確保方法。

９．さらに、送付する電子情報の原本を保存し、受信者側で受信した情報ブロックを返送させ、前記電子情報原本と照合して同一性を確認することを特徴とする請求の範囲第５項から第７項のいずれかに記載の電子情報の安全確保方法。

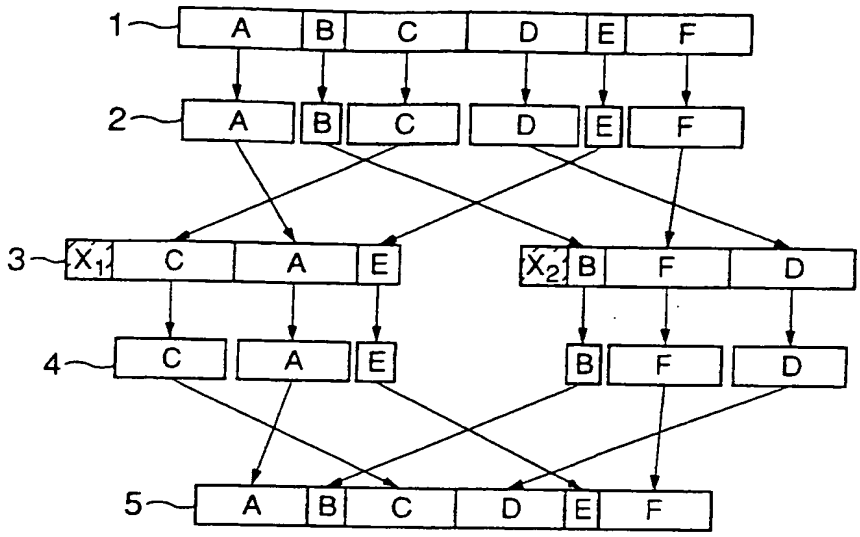
１０．前記情報ブロックおよび前記分割抽出データのうち少なくとも１個が他の電子情報の伝送手段と異なる第２の伝送手段により受信者に送付されることを特徴とする請求の範囲第５項から第９項のいずれかに記載の電子情報の安全確保方法。

１１．前記伝送手段または第２伝送手段には転送局を介在させて、該伝送手段で送る情報のブロックは宛先情報と共に情報パッケージに収容して該転送局に宛てて送付し、該転送局が該宛先情報に基づいて前記受信者に転送することを特徴とする請求の範囲第１０項記載の電子情報の安全確保方法。

１２．前記転送局が前記情報ブロックを前記受信者の請求があるまで格納保持していることを特徴とする請求の範囲第１１項記載の電子情報の安全確保方法。

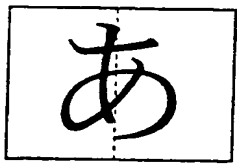
１３．電子情報ファイルを分割した前記情報ブロックを証明局と当事者がそれぞれ分かち持つようにして、該電子情報を使用するときに該証明局と該当事者とからすべての前記情報ブロックを収集して統合し、元の電子情報を復元することを特徴とする請求の範囲第１項から第１２項のいずれかに記載の電子情報の安全性確保方法。

第１図

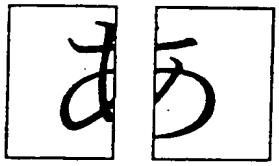


第２図

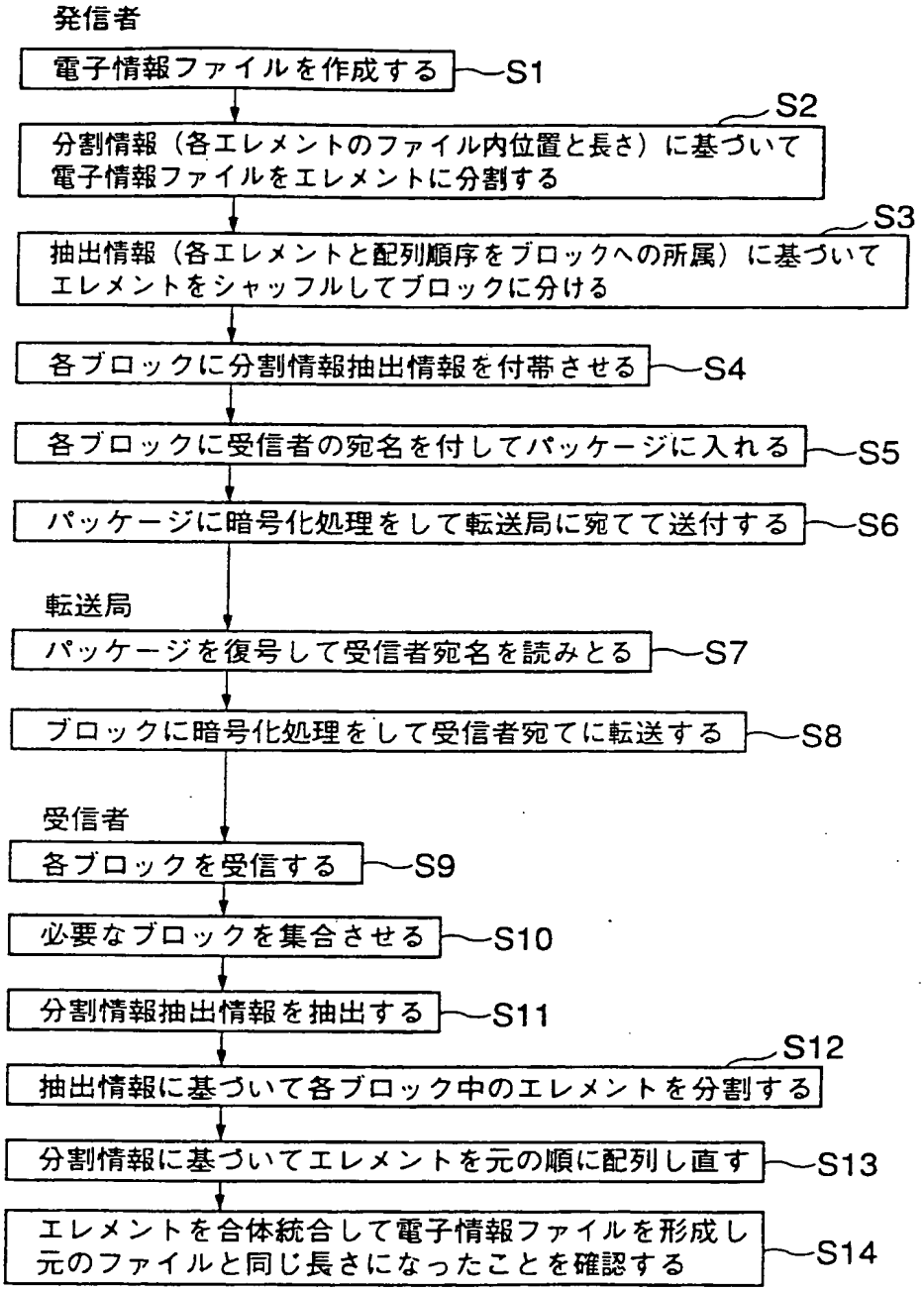
(a)



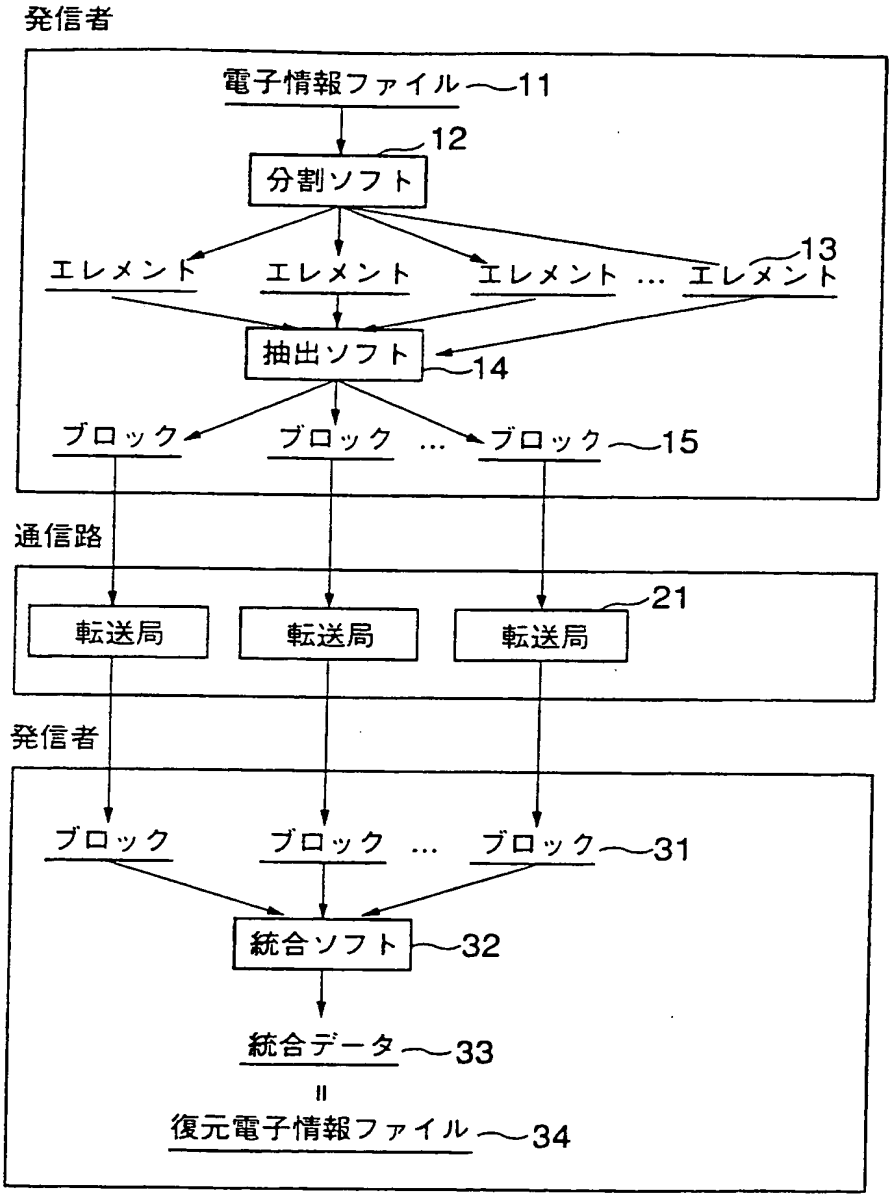
(b)



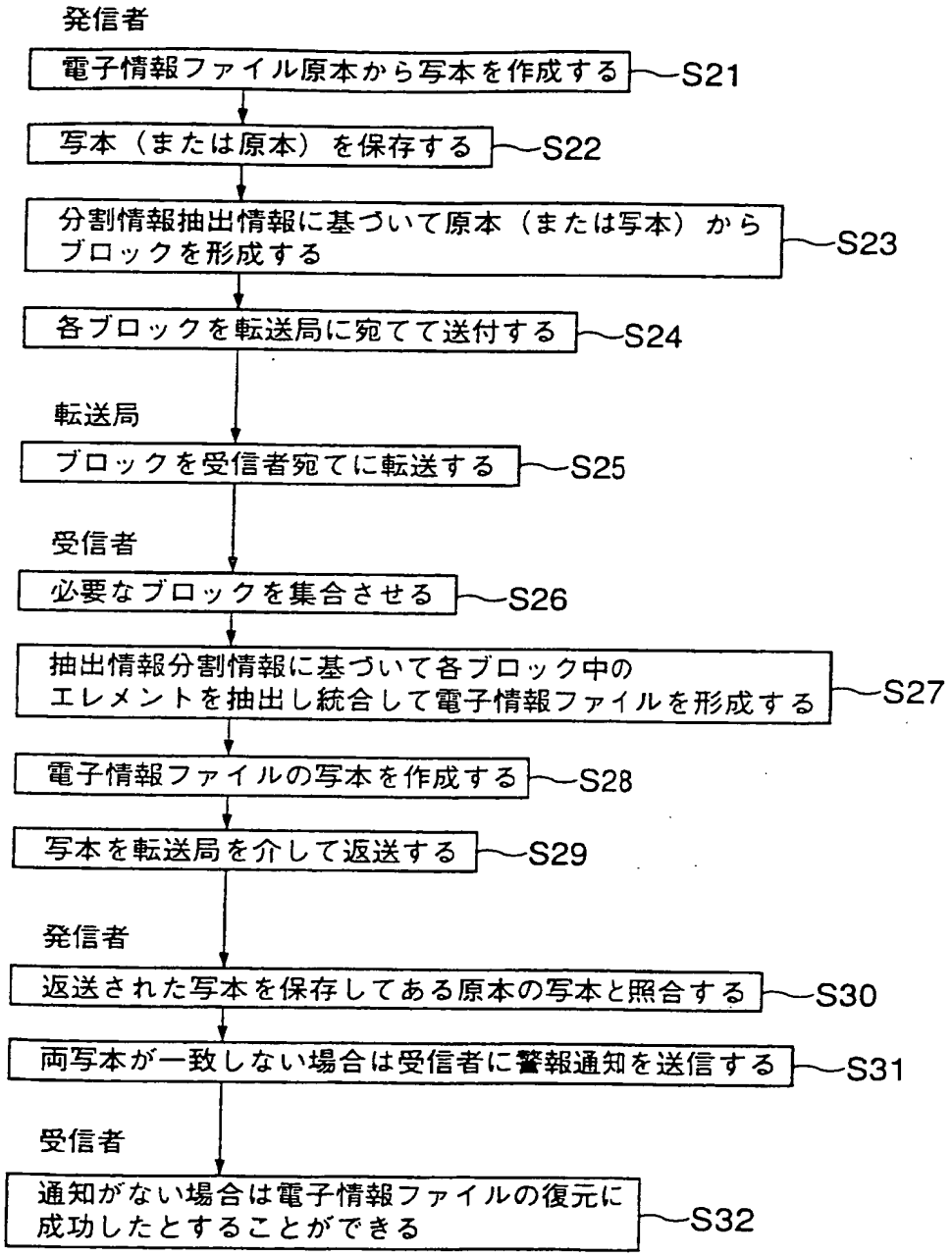
第３図


発信者
電子情報ファイルを作成する
S1
分割情報（各エレメントのファイル内位置と長さ）に基づいて電子情報ファイルをエレメントに分割する
S2
抽出情報（各エレメントと配列順序をブロックへの所属）に基づいてエレメントをシャッフルしてブロックに分ける
S3
各ブロックに分割情報抽出情報を付帯させる
S4
各ブロックに受信者の宛名を付してパッケージに入れる
S5
パッケージに暗号化処理をして転送局に宛てて送付する
S6
転送局
パッケージを復号して受信者宛名を読みとる
S7
ブロックに暗号化処理をして受信者宛てに転送する
S8
受信者
各ブロックを受信する
S9
必要なブロックを集合させる
S10
分割情報抽出情報を抽出する
S11
抽出情報に基づいて各ブロック中のエレメントを分割する
S12
分割情報に基づいてエレメントを元の順に配列し直す
S13
エレメントを合体統合して電子情報ファイルを形成し元のファイルと同じ長さになったことを確認する
S14

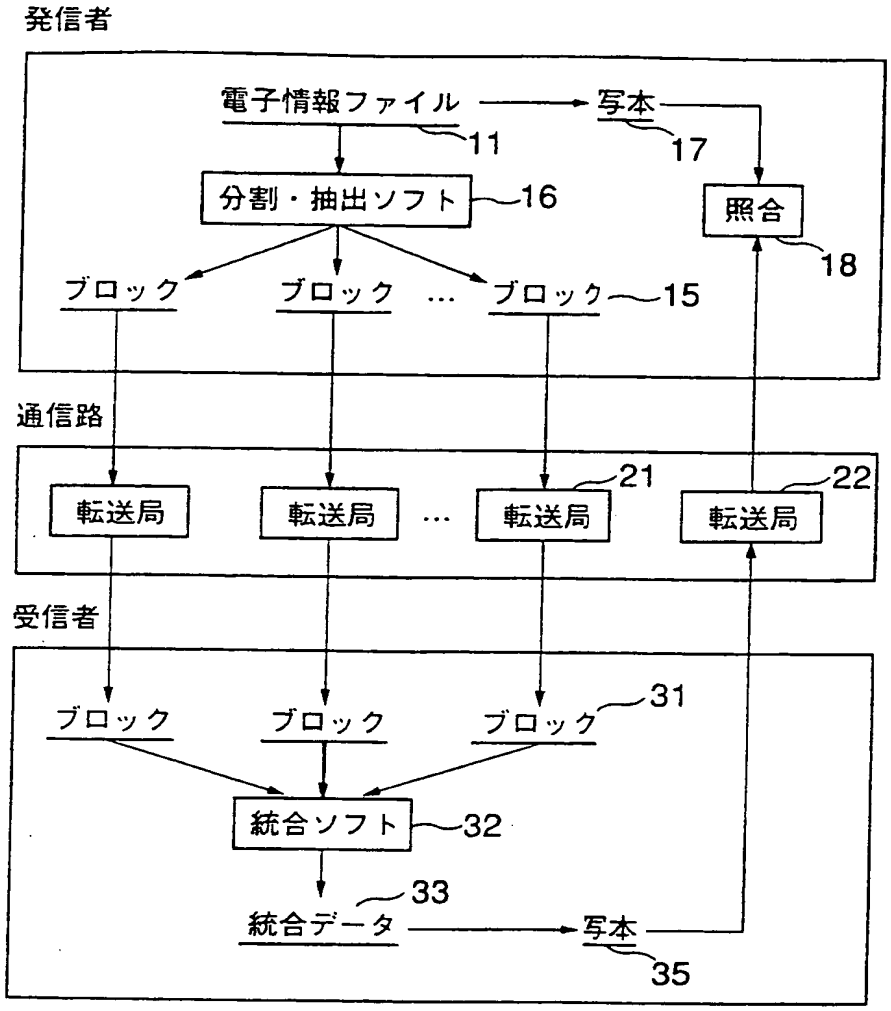
第４図


発信者
電子情報ファイル
11
12
分割ソフト
エレメント
エレメント
エレメント
エレメント
13
抽出ソフト
14
ブロック
ブロック
ブロック
15
通信路
転送局
転送局
転送局
21
発信者
ブロック
ブロック
ブロック
31
統合ソフト
32
統合データ
33
復元電子情報ファイル
34

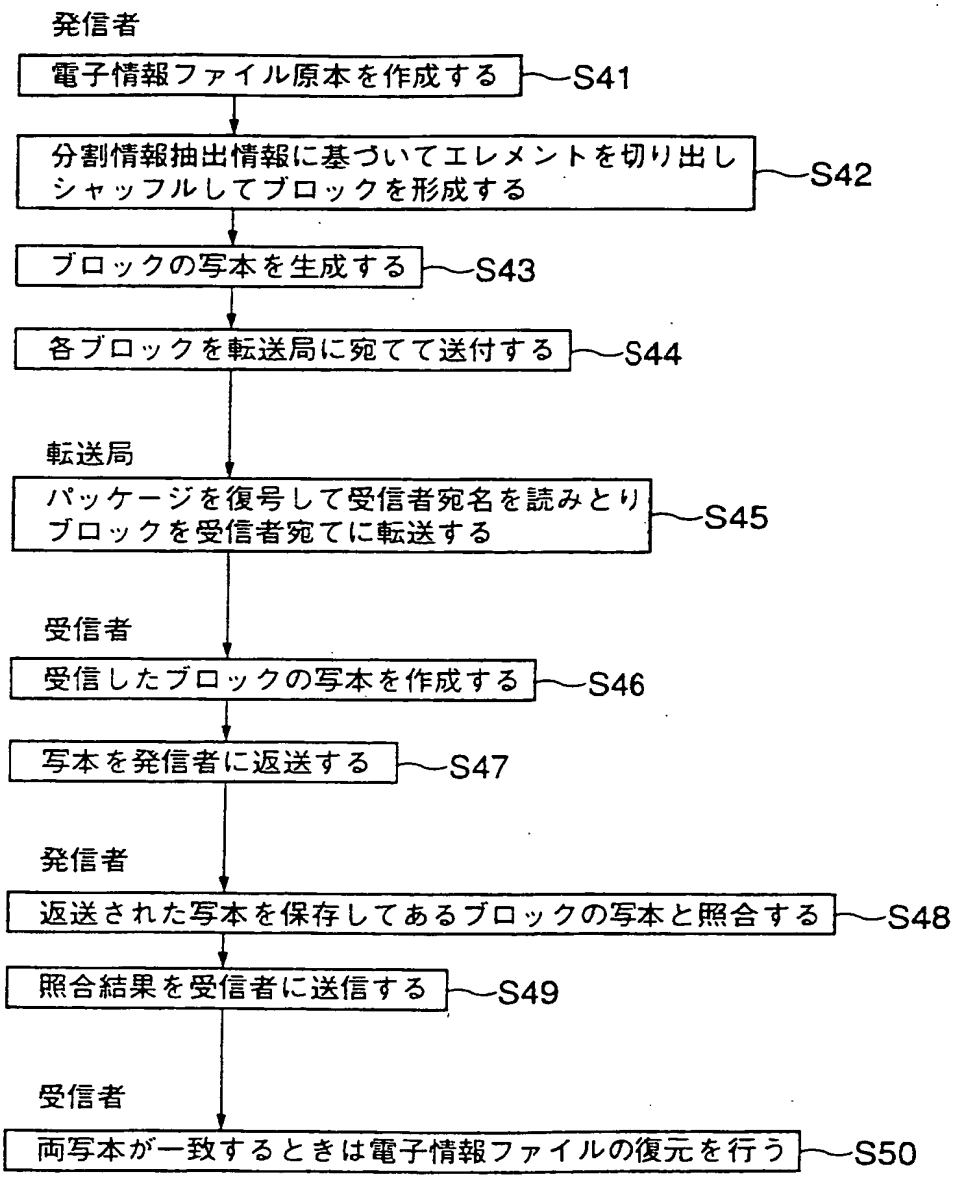
第５図


発信者
電子情報ファイル原本から写本を作成する
S21
写本（または原本）を保存する
S22
分割情報抽出情報に基づいて原本（または写本）から
ブロックを形成する
S23
各ブロックを転送局に宛てて送付する
S24
転送局
ブロックを受信者宛てに転送する
S25
受信者
必要なブロックを集合させる
S26
抽出情報分割情報に基づいて各ブロック中の
エレメントを抽出し統合して電子情報ファイルを形成する
S27
電子情報ファイルの写本を作成する
S28
写本を転送局を介して返送する
S29
発信者
返送された写本を保存してある原本の写本と照合する
S30
両写本が一致しない場合は受信者に警報通知を送信する
S31
受信者
通知がない場合は電子情報ファイルの復元に
成功したとすることができる
S32

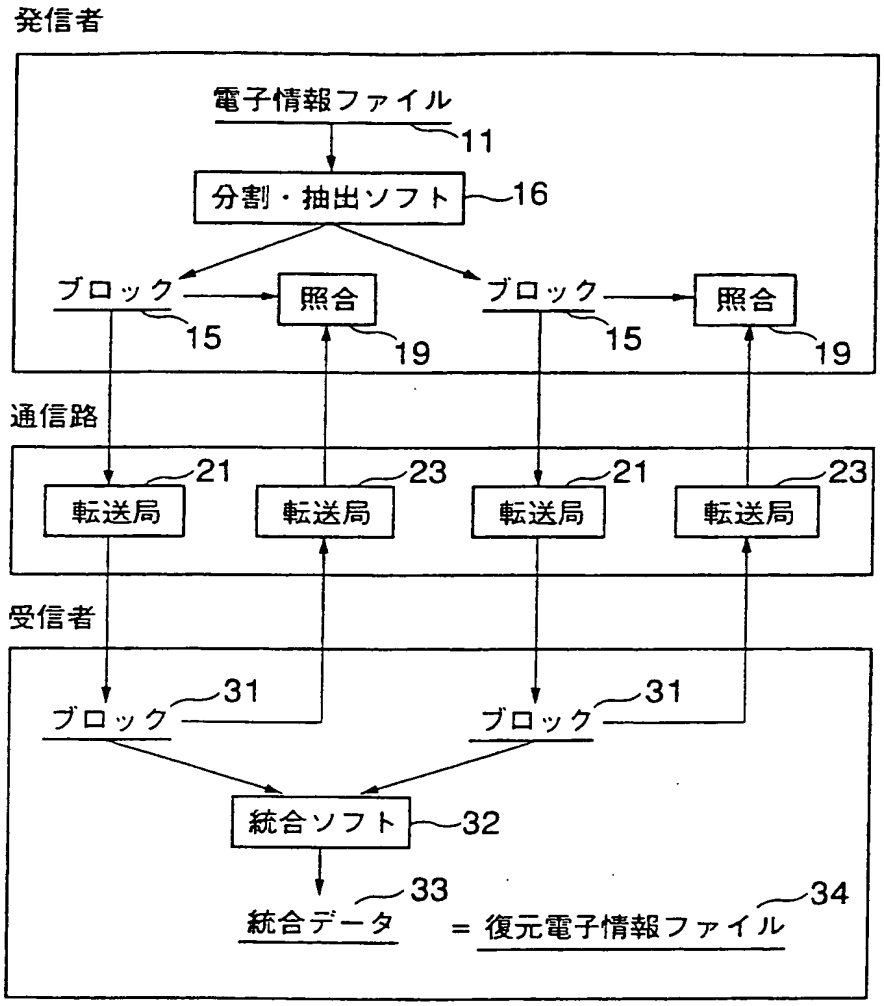
第６図


発信者
電子情報ファイル
11
写本
17
分割・抽出ソフト
16
照合
18
ブロック
ブロック
…
ブロック
15
通信路
転送局
転送局
…
転送局
21
転送局
22
受信者
ブロック
ブロック
ブロック
31
統合ソフト
32
33
統合データ
写本
35

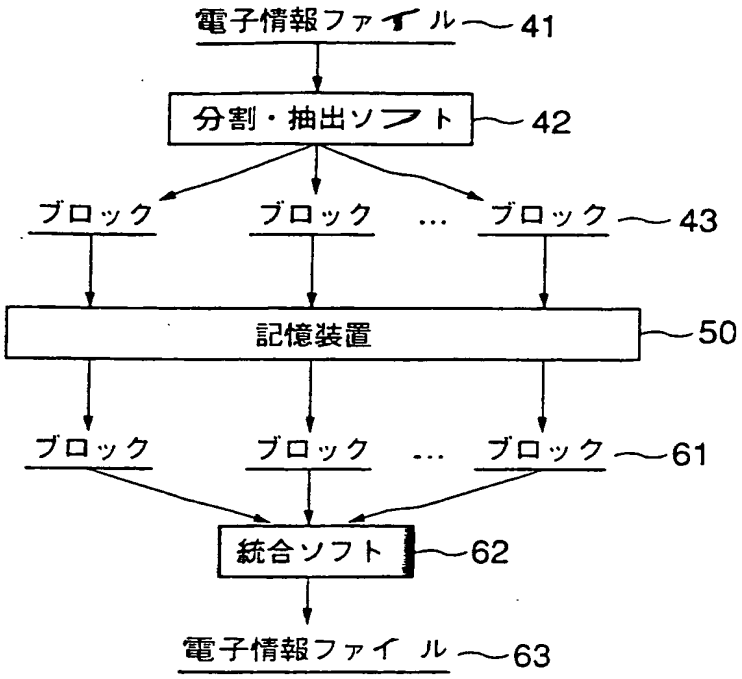
第７図


発信者
電子情報ファイル原本を作成する
S41
分割情報抽出情報に基づいてエレメントを切り出し
シャッフルしてブロックを形成する
S42
ブロックの写本を生成する
S43
各ブロックを転送局に宛てて送付する
S44
転送局
パッケージを復号して受信者宛名を読みとり
ブロックを受信者宛てに転送する
S45
受信者
受信したブロックの写本を作成する
S46
写本を発信者に返送する
S47
発信者
返送された写本を保存してあるブロックの写本と照合する
S48
照合結果を受信者に送信する
S49
受信者
両写本が一致するときは電子情報ファイルの復元を行う
S50

第８図


発信者
電子情報ファイル
11
分割・抽出ソフト
16
ブロック
15
照合
19
ブロック
15
照合
19
通信路
21
転送局
23
転送局
21
転送局
23
転送局
受信者
31
ブロック
31
ブロック
統合ソフト
32
33
統合データ
= 復元電子情報ファイル
34

第９図


電子情報ファイル
41
分割・抽出ソフト
42
ブロック
ブロック
…
ブロック
43
記憶装置
50
ブロック
ブロック
…
ブロック
61
統合ソフト
62
電子情報ファイル
63